Quaternion Algebras

Preliminary Arizona Winter School, 2026

Jen Berg
Department of Mathematics and Statistics, Bucknell University
jsb047@bucknell.edu

September 18, 2026

Introduction

Welcome!

These notes about quaternion algebras are written for the Preliminary Arizona Winter School in 2026 and aimed at an audience of undergraduates with a first course in abstract algebra. If that does not describe you, then that doesn't mean these notes aren't for you! However, you may want to brush up on a few concepts from linear and abstract algebra including bases, dimension, ideals, ring homomorphisms, field extensions, and finite fields. Algebra texts such as [DF04, Chapters 7,8] or [Sil22, Chapters 3–5] are a great place to start.

The notes are meant to be self contained, but I hope that they will spark your curiosity and you will feel inspired to explore this beautiful subject more deeply. Some textbook references that you might find helpful as a starting point include [GS17, Ser73, Voi21], although all of these are at the graduate level. Another source freely available online is [Conb] which was also invaluable to me while writing these notes.

Scope

Quaternion algebras are a vast subject. These notes take a somewhat narrow perspective with an eye towards the topic of the 2026 Arizona Winter School: Rationality and Irrationality: Arithmetic and Geometry. These notes introduce quaternion algebras from an algebraic perspective with a goal of distinguishing between quaternion algebras over the rational numbers via arithmetic and geometry. Five lectures is short! There are many aspects of quaternion algebras that we must skip. One that may be of interest to the casual reader is their connections to visualizations; see for example [Han06, Chapters 1 and 2].

What will we cover?

Here is a brief roadmap of what we'll cover in the five lectures:

- **Lecture 1 (Hamilton quaternions and foundations):** We start with Hamilton's quaternions $\mathbb{H}$ as historical motivation before generalizing to arbitrary quaternion algebras $(a,b)_F$ over a base field F.
- **Lecture 2 (Isomorphisms, bases, and splitting):** We characterize when two quaternion algebras are isomorphic and explore the concept of *splitting*—determining when $(a,b)_F \cong M_2(F)$ versus when it remains a division algebra.
- **Lecture 3 (Central simple algebras & associated conics):** We place quaternion algebras into the broader context of central simple algebras (CSAs) and establish a connection between algebra and geometry by associating a conic curve to each quaternion algebra.
- **Lecture 4 (A primer on p-adics):** We introduce the p-adic integers $\mathbb{Z}_p$, p-adic valuations to give us the machinery needed to understand behavior of quaternion algebras over the rational numbers in the final lecture.
- **Lecture 5 (Quaternion algebras over $\mathbb{Q}$):** We define a tool called the Hilbert symbol $(a,b)_p$ and apply a local-global principle to distinguish non-isomorphic quaternion algebras over $\mathbb{Q}$.

How should you use these notes?

As many others have probably said before me, mathematics is not a spectator sport! Even reading mathematics should be active rather than passive. When you encounter a new definition, try working through an example. Challenge yourself to come up with your own example or instructive non-example. Additionally, you should make some time to work through the inline exercises scattered throughout the text (which are distinct from the problem sets accompanying the course).

What if you find a typo?

I hope there won't be many, but inevitably there will be some. Just send me an email. I appreciate it!

Acknowledgements

Many thanks to the PAWS organizers without whom this course would not be possible. Thank you to the problem session leaders Matt Broe, Xinyu Fang, Divyasree Ramachandran, and Alex Wang for all of their hard work, careful reading, and feedback.

Contents

Lecture 1: Hamilton quaternions and foundations

1.1 Motivation

The construction of the complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ provides a bridge between algebra and geometry. In the 2-dimensional plane, addition of complex numbers corresponds to vector addition or translation, while multiplication encodes scaling and rotations. For instance, multiplying a vector by i corresponds to a $90°$ rotation.

Given the correspondence between planar rotations and multiplication in the complex numbers, a natural question arises. Can we construct a similar 3-dimensional algebra to model rotations in 3-dimensional space? William Rowan Hamilton spent over a decade searching for such a system (from roughly 1830 until his breakthrough on October 16, 1843). He eventually realized that a 3-dimensional associative division algebra over $\mathbb{R}$ is an algebraic impossibility. To preserve the ability to divide by non-zero elements while extending the complex numbers, we must make a structural compromise. By expanding the construction to a 4-dimensional algebra and dropping the axiom of commutativity, Hamilton arrived at the quaternions, denoted $\mathbb{H}$. This algebra serves as our archetypal example of a non-commutative division ring and forms the foundation for the general theory of quaternion algebras we will develop in this course.

1.2 Hamilton's quaternions

Definition 1.1: Hamilton Quaternions

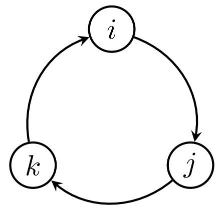
The **(Hamilton) quaternions** *are*

$$\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

with multiplication defined by the relations

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad \text{and every } a \in \mathbb{R} \text{ commutes with } i, j, k.$$

Just as the complex numbers form a 2-dimensional $\mathbb{R}$-vector space with basis $\{1, i\}$, the Hamilton quaternions form a 4-dimensional $\mathbb{R}$-vector space spanned by $\{1, i, j, k\}$. Equipped with the multiplication rules above, $\mathbb{H}$ becomes an associative ring. A helpful way to remember the rules for multiplication in $\mathbb{H}$ is to arrange i, j, k clockwise in a circle. Moving along the arrows gives a positive product (e.g., $ij = k$, $jk = i$, $ki = j$), while moving against the arrows gives a negative product (e.g., $ji = -k$, $kj = -i$, $ik = -j$).



The rules for multiplication among i, j, k together with the distributive law are all we need to multiply any elements in $\mathbb{H}$.

Example 1.2. $(i + 2j)(2i - j) = 2i^2 - ij + 4ji - 2j^2 = -2 - k - 4k - (-2) = -5k$.

Before proving structural properties, it is helpful to get some hands-on practice calculating directly with elements in $\mathbb{H}$.

Exercise 1.3. Let $q = 1 + 2i - j$ and $r = 2i + k$ be quaternions in $\mathbb{H}$.

(i) Compute the products qr and rq. Verify explicitly that $qr \neq rq$.

(ii) Calculate q^2 and r^2.

(iii) Compute $(q + r)(q - r)$ and compare it to $q^2 - r^2$. Why are these two expressions not equal in $\mathbb{H}$?

To get a better sense of how non-commutativity controls arithmetic in $\mathbb{H}$, we can ask: which quaternions still commute with every element, and how many square roots of -1 exist?

Exercise 1.4.

(i) The **center** of $\mathbb{H}$ is defined as $Z(\mathbb{H}) = \{q \in \mathbb{H} \mid qx = xq \text{ for all } x \in \mathbb{H}\}$. Prove that $Z(\mathbb{H}) = \mathbb{R}$. *(Hint: Write $q = a + bi + cj + dk$ and compute $qi - iq$ and $qj - jq$.)*

(ii) Find all **pure quaternions**, i.e., elements of the form $q = bi + cj + dk$, that satisfy $q^2 = -1$. How does your result compare with the complex numbers $\mathbb{C}$?

The Hamilton quaternions $\mathbb{H}$ are built over the real numbers with $i^2 = j^2 = -1$. However, we can abstract this construction by replacing $\mathbb{R}$ with an arbitrary base field F, and allowing i^2 and j^2 to equal any non-zero scalars $a, b \in F^\times$. While $\mathbb{H}$ is optimized for geometry over $\mathbb{R}$, extending this framework to other fields including the rational numbers or finite fields turns out to give us a powerful tool in number theory.

In these settings, quaternion algebras provide arithmetic machinery used to study quadratic forms, prime factorization, and the classification of non-commutative rings. This leads us directly to our general definition.

1.3 General quaternion algebras

From now on, F is assumed to be field with characteristic not equal to 2.

Definition 1.5: Quaternion algebra

Let F be a field and let $a, b \in F^\times$. The **quaternion algebra** $(a,b)_F$ *is the 4-dimensional F-algebra with basis $\{1, i, j, ij\}$ and multiplication determined by the relations*

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Remark 1.6. *Let's clarify two pieces of terminology we'll use throughout these notes:*

- *An F-***algebra** *A is both an F-vector space and a ring, where scalar multiplication and ring multiplication are compatible, i.e.,*

$$(cx)(dy) = (cd)(xy) \quad \text{for all } c, d \in F \text{ and } x, y \in A.$$

- *A* **division algebra over** *F is an F-algebra D in which every non-zero element $v \in D$ has a multiplicative inverse $v^{-1} \in D$.*

Note: A division algebra is simply a field if multiplication is commutative, or a non-commutative "skew field" like $\mathbb{H}$ if it is not.

Aside 1.7. *Why do we enforce* $\mathrm{char}(F) \neq 2$*? Recall that in a field of characteristic 2, we have $1 + 1 = 0$, which implies $1 = -1$. If we allowed $\mathrm{char}(F) = 2$, our core non-commutative relation $ij = -ji$ would become $ij = ji$. The algebra would become a commutative ring! It is worth noting that quaternion algebras* do *exist in characteristic 2, but they require a completely different set of structural relations (namely, $i^2 + i = a$, $j^2 = b$, and $ji = (i + 1)j$) to preserve non-commutativity. We will leave the characteristic 2 setting aside for this course, but the interested reader should consult [GS17, Section 1.2] for further details.*

Example 1.8 (Quaternion algebras over $\mathbb{Q}$)**.** *By varying the parameters $a, b \in \mathbb{Q}^\times$, we obtain different 4-dimensional algebras over the rational numbers:*

- *In $(-1,-1)_\mathbb{Q}$, we have $i^2 = -1$ and $j^2 = -1$. This is simply Hamilton's quaternions restricted to rational coordinates $a, b, c, d \in \mathbb{Q}$.*
- *In $(2,3)_\mathbb{Q}$, we have $i^2 = 2$, $j^2 = 3$, and $ij = -ji$. An element looks like $v = v_0 + v_1 i + v_2 j + v_3 ij$ with $v_k \in \mathbb{Q}$, where $ij \cdot ij = (ij)(-ji) = -i(jj)i = -i(3)i = -3i^2 = -6$.*

To study the structure of general quaternion algebras, we need an algebraic mechanism to extract scalar quantities from quaternion elements. Recall that for a complex number $z = x+iy$, multiplying by its complex conjugate $\overline{z} = x - iy$ yields a real number, $|z|^2 = x^2 + y^2$, which measures its squared magnitude. We can generalize this construction to any quaternion algebra $(a,b)_F$ by defining a conjugation map that allows us to recover an element of the base field F via multiplication, giving us an algebraic analogue of squared magnitude known as the *norm*.

Definition 1.9: Conjugate and Norm

Let $v = v_0 + v_1 i + v_2 j + v_3 ij$ be an element of the quaternion algebra $(a,b)_F$. The **conjugate** *of v is*

$$\overline{v} := v_0 - v_1 i - v_2 j - v_3 ij$$

and the **norm** *of v is*

$$N(v) := v\overline{v} = v_0^2 - a v_1^2 - b v_2^2 + ab v_3^2.$$

The map $(a,b)_F \to (a,b)_F$ defined by $v \mapsto \overline{v}$ is called an **anti-automorphism** of the F-algebra $(a,b)_F$, which means it is an F-vector space isomorphism of $(a,b)_F$ satisfying $vw \mapsto \overline{vw} = \overline{w}\,\overline{v}$. Moreover $\overline{\overline{v}} = v$, and an anti-automorphism with this property is called an **involution** in ring theory. For more information about involutions and central simple algebras, see [KMRT98].

Proposition 1.10: Invertible elements in quaternion algebras

An element q of the quaternion algebra $(a,b)_F$ is invertible if and only if it has nonzero norm. In particular, $(a,b)_F$ is a division algebra if and only if the norm $N\colon (a,b)_F \to F$ does not vanish except at 0.

Proof. The norm is a multiplicative function since

$$N(q_1q_2) = q_1q_2\overline{(q_1q_2)} = q_1q_2\ \overline{q_2}\ \overline{q_1} = q_1 N(q_2)\overline{q_1} = q_1\overline{q_1}N(q_2) = N(q_1)N(q_2).$$

(Since $N(q_2) \in F$ is a scalar in the base field, it commutes with the quaternion $\overline{q_1}$.)

If $qq' = 1$ for some element q' then $N(q)N(q') = N(1) = 1$ in F thus $N(q) \neq 0$. Conversely, if $N(q) \neq 0$, the quaternion $\overline{q}/N(q)$ is a two-sided multiplicative inverse for q. □

Proposition 1.10 provides a straightforward algebraic criterion for invertibilty. To see this in action, we can ask whether the norm can actually vanish for a non-zero element, or if every quaternion algebra is automatically a division algebra. The following example demonstrates that the norm can indeed vanish, even over familiar fields like the rational numbers.

Example 1.11. *Consider the quaternion algebra $A = (1, -1)_{\mathbb{Q}}$, where $i^2 = 1$ and $j^2 = -1$. Let's examine the element $v = 1 + i$. Its norm is*

$$N(1 + i) = (1 + i)(1 - i) = 1 - i + i - i^2 = 1 - 1 = 0.$$

Since $N(v) = 0$ but $v \neq 0$, Proposition 1.10 tells us that $1 + i$ is not invertible. In fact, it is a zero divisor! Thus, $(1, -1)_{\mathbb{Q}}$ is an example of a quaternion algebra that is not a division algebra.

Exercise 1.12. For each of the following quaternion algebras, determine whether it is a division algebra or not. Justify your answer either by demonstrating that the norm map has no non-trivial zeros or by explicitly constructing a non-zero zero divisor.

(i) $A_1 = (-1, -1)_{\mathbb{R}}$ (The classical Hamilton quaternions $\mathbb{H}$)

(ii) $A_2 = (2, 2)_{\mathbb{Q}}$

(iii) $A_3 = (1, 5)_{\mathbb{Q}}$

(iv) Come up with your own examples!

Hint: For (i), inspect the signs of the coefficients in the norm form. For (ii) and (iii), write out the norm form and look for small integer choices for v_0, v_1, v_2, v_3 that cause the terms to cancel out to zero.

Looking Ahead

In this introductory lecture, we have established the foundational structure of quaternion algebras and observed that their algebraic structure is closely tied to the behavior of the quadratic norm form $N(v)$. Specifically, Proposition 1.10 shows that whether an algebra admits a division ring structure depends entirely on whether the equation $N(v) = 0$ has non-trivial solutions.

In the next lecture, we will show that the presence of these non-zero zero divisors implies that the algebra is isomorphic to the matrix ring $M_2(F)$, a property known as being *split*. This sets up the central theme of the course: classifying quaternion algebras up to isomorphism over various base fields. We will achieve this by translating our algebraic questions into a geometric setting, where finding zero divisors corresponds to finding solutions to an equation that defines a curve. From there, we will explore the behavior of quaternion algebras over finite fields, and eventually introduce specialized number systems called p-adic fields that allow us to study arithmetic one prime number at a time. Ultimately, we will see how combining this "localized" information allows us to determine the behavior of a quaternion algebra over the rational numbers.

Key Takeaways

Non-commutativity: Extending the complex numbers to a 3-dimensional associative division algebra over $\mathbb{R}$ is not possible. To build a higher-dimensional analogue of $\mathbb{C}$ with these properties, we must expand to 4 dimensions and drop commutativity ($ij = -ji$).

Algebra is governed by arithmetic: A general quaternion algebra $(a, b)_F$ is a division ring if and only if its associated norm form $N(v) = v_0^2 - av_1^2 - bv_2^2 + abv_3^2$ has no non-trivial zeros.

Lecture 2: Isomorphisms, bases, and splitting

To begin classifying quaternion algebras, we must first make precise what it means for two algebras to have the same structure. Because these algebras are built directly over a base field F, a meaningful structural mapping must preserve not only the ring operations but also the underlying scalar action of F. This motivates our formal definition of an algebra isomorphism.

2.1 Isomorphisms of quaternion algebras

Definition 2.1: Isomorphism of quaternion algebras

A **isomorphism** *between two (quaternion) algebras A and A' over F is a ring isomorphism $\varphi\colon A \xrightarrow{\sim} A'$ that fixes the elements of F, i.e., $\varphi(c) = c$ for all $c \in F$.*

It turns out that the isomorphism class of the quaternion algebra $(a, b)_F$ depends only on the classes of a and b in $F^\times/F^{\times 2}$. In order to make sense of this statement, we can use a particular type of basis to show that two quaternion algebras are isomorphic.

Definition 2.2: Quaternionic basis

A basis of $(a, b)_F$ of the form $\{1, u, v, uv\}$ with $u^2 \in F^\times$, $v^2 \in F^\times$, and $uv = -vu$ is called a **quaternionic basis** *of $(a, b)_F$.*

The notion of quaternionic basis gives some immediate isomorphisms between different quaternion algebras. Since the sets below are formed by scaling and swapping the original basis vectors, they automatically remain bases, though you should check for yourself to see how the new parameters emerge!

1. Since $\{1, i, j, ij\}$ is a quaternionic basis for $(a, b)_F$ (where $i^2 = a$, $j^2 = b$ and $ij = -ji$), so too is $\{1, j, i, ji\}$. Thus $(a, b)_F \cong (b, a)_F$.

2. Similarly, $\{1, i, ij, aj\} = \{1, i, ij, i^2 j\}$ is a quaternionic basis for $(a, b)_F$. Hence $(a, b)_F \cong (a, -ab)_F$.

3. Similarly, $\{1, j, ij, -bi\} = \{1, j, ij, jij\}$ is a quaternionic basis for $(a, b)_F$. Hence $(a, b)_F \cong (b, -ab)_F$.

4. Finally, $\{1, ci, dj, cdij\}$ is a quaternionic basis of $(a, b)_F$ for all $c, d \in F^\times$. Thus $(a, b)_F \cong (ac^2, bd^2)_F$ for all nonzero $c, d \in F$.

In particular, note that taking $b = 1$ in (2) above gives $(a, 1)_F \cong (a, -a)_F$, while $b = -1$ yields $(a, -1)_F \cong (a, a)_F$. Up to isomorphism, the algebra $(a, b)_F$ depends on a, b only up to multiplication by nonzero squares in F; we have $(a, c^2)_F = (a, 1)_F = (1, a)_F$ and $(c^2, b)_F = (1, b)_F$.

We can summarize the discussion above in the following useful corollary.

Corollary 2.3

Let $a, b \in F^\times$. The isomorphism class of $(a, b)_F$ satisfies:

1. $(a, b)_F \cong (b, a)_F$.
2. $(a, b)_F \cong (a, -ab)_F \cong (b, -ab)_F$.
3. $(a, b)_F \cong (ac^2, bd^2)_F$ *for all* $c, d \in F^\times$.
4. $(ca, cb)_F \cong (-ab, ca)_F$ *for all* $c \in F^\times$.

The preceding examples show how changing a known basis alters the parameters a and b. The following exercise demonstrates that, conversely, any four elements satisfying the relations in Definition 2.2 automatically yield a valid basis.

Exercise 2.4. ([Conb]) Given $u, v \in (a, b)_F$ such that u, v are not in F but $u^2 \in F^\times$, $v^2 \in F^\times$, and $uv = -vu$, show that $\{1, u, v, uv\}$ is a linearly independent set and hence is a quaternionic basis of $(a, b)_F$.

(Hint: Recall $\mathrm{char}(F) \neq 2$. One approach is to show first that $\{1, u\}$ is independent. Then $\{1, u, v\}$ using $uv = -vu$ and $u^2 \in F^\times$, and finally $\{1, u, v, uv\}$ using $u^2, v^2 \in F^\times$ and $uv = -vu$.)

The next result shows that $M_2(F)$, the algebra of 2×2 matrices over F, is a quaternion algebra over F. In particular, any quaternion algebra $(a, b)_F$ where a or b is a square (such as $(a, c^2)_F$) is isomorphic to $M_2(F)$.

Proposition 2.5: $M_2(F)$ is a quaternion algebra

For all $a \in F^\times$, there is an isomorphism of F-algbras $(1, a)_F \cong M_2(F)$.

Proof. Let $\{1, i, j, ij\}$ be a basis for $(1, a)_F$. Consider the map $\varphi\colon (1, a)_F \to M_2(F)$ defined by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad ij \mapsto \begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix},$$

and extend F-linearly to obtain:

$$v_0 + v_1 i + v_2 j + v_3 ij \mapsto \begin{pmatrix} v_0 + v_1 & a(v_2 + v_3) \\ v_2 - v_3 & v_0 - v_1 \end{pmatrix}.$$

The image of $1, i, j, ij$ in $M_2(F)$ forms a linearly independent set of size $4 = \dim(M_2(F))$ so the map is a bijection. It fixes $c \in F$ since $c \mapsto \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$. Finally, one can verify that the map φ is multiplicative. $\square$

Exercise 2.6. Verify that the map φ defined in Proposition 2.5 is indeed multiplicative and the image of $1, i, j, ij$ forms a linearly independent set.

Because $M_2(F)$ contains matrices that square to zero (nilpotents) or square to themselves (idempotents), we can use the isomorphism φ to construct explicit zero-divisors and elements satisfying $e^2 = e$ directly inside the quaternion algebra $(1, a)_F$.

Exercise 2.7. Let $\varphi\colon (1, a)_F \xrightarrow{\sim} M_2(F)$ be the isomorphism defined in Proposition 2.5.

(i) Find the unique element $v \in (1, a)_F$ such that $\varphi(v) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

(ii) Verify directly in $(1, a)_F$ that $v^2 = 0$.

(iii) Find the unique element $e \in (1, a)_F$ such that $\varphi(e) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, and verify directly that $e^2 = e$.

2.2 Splitting of quaternion algebras

This relationship between a quaternion algebra and a matrix ring is a fundamental structural property that we will study across different fields. We define this behavior explicitly below.

Definition 2.8: Split quaternion algebra

A quaternion algebra over F is called **split** *if it is isomorphic to $M_2(F)$ as an F-algebra.*

Example 2.9. *Up to isomorphism, there are only two quaternion algebras over $F = \mathbb{R}$ and one quaternion algebra over $F = \mathbb{C}$. In particular, since $\mathbb{R}^\times/\mathbb{R}^{\times 2} \cong \{\pm 1\}$,*

$$(a,b)_{\mathbb{R}} \cong \begin{cases} \mathbb{H} = (-1,-1)_{\mathbb{R}}, & \text{if } a \text{ and } b \text{ are negative} \\ M_2(\mathbb{R}), & \text{if } a \text{ or } b \text{ is positive,} \end{cases}$$

and all elements of $\mathbb{C}^\times$ are squares in $\mathbb{C}$, so $(a,b)_{\mathbb{C}} \cong M_2(\mathbb{C})$ for all $a, b \in \mathbb{C}^\times$. That is, all quaternion algebras over $\mathbb{C}$ are split.

Over $F = \mathbb{Q}$, however, the situation is quite different. We shall see that there are infinitely many non-isomorphic quaternion algebras over $\mathbb{Q}$.

So far, we've seen that a simple condition that guarantees $(a,b)_F$ is split is to have $b \in F^{\times 2}$. However, this condition can be weakened to obtain other quaternion algebras that are split. First, we'll need to understand a particular subgroup of elements of $F^\times$.

Lemma 2.10

For $a \in F^\times$, the set of nonzero elements $x^2 - ay^2$ with $x, y \in F$ is a subgroup of $F^\times$.

Recall that if a is not a square in $F^\times$, then $F(\sqrt{a}) = \{x + \sqrt{a}y \mid x, y \in F\}$ is a field and is isomorphic to the quotient $F(\sqrt{a}) \cong F[t]/(t^2 - a)$. The map $N_{F(\sqrt{a})/F} \colon F(\sqrt{a})^\times \to F^\times$ defined by $x + \sqrt{a}y \mapsto x^2 - ay^2$ is a homomorphism of multiplicative groups. Therefore the image $N_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)$ is a subgroup of $F^\times$. We will verify Lemma 2.10 directly, however.

Proof of Lemma 2.10. Let $N_a \coloneqq \{x^2 - ay^2 | x, y \in F\} \setminus \{0\}$. Then $1 \in N_a$ since we can take $x = 1$ and $y = 0$. N_a is closed under multiplication since

$$(x_1^2 - ay_1^2)(x_2^2 - ay_2^2) = (x_1x_2 + ay_1y_2)^2 - a(x_1y_2 + x_2y_1)^2.$$

Finally, N_a is closed under inversion since

$$\frac{1}{x^2 - ay^2} = \frac{x^2 - ay^2}{(x^2 - ay^2)^2} = \left(\frac{x}{x^2 - ay^2}\right)^2 - a\left(\frac{y}{x^2 - ay^2}\right)^2.$$

□

Observe that N_a always contains the subgroup $F^{\times 2}$ of all squares in $F^\times$ by taking $y = 0$. When a is a square, the set N_a contains all of $F^\times$.

Lemma 2.11

If a is a square in F, then $N_a = F^\times$.

Proof. Suppose $a = c^2$ for $c \in F^\times$. Then for any $x, y \in F$ we have

$$x^2 - ay^2 = x^2 - c^2y^2 = (x - cy)(x + cy).$$

Letting $u = x + cy$ and $v = x - cy$ we have $x = \frac{u+v}{2}$ and $y = \frac{u-v}{2c}$ (recall, $\mathrm{char}(F) \neq 2$ and $c \neq 0$ so this is an invertible linear change of variables). For any $b \in F^\times$, set $u = 1$ and $v = b$, gives $x = \frac{1+b}{2}$ and $y = \frac{1-b}{2c}$ so that $x^2 - ay^2 = b$. □

With these lemmas in hand, we are ready to give several equivalent characterizations of splitness.

Theorem 2.12: Characterizations of splitness

The following are equivalent for a quaternion algebra $(a, b)_F$.

1. *The algebra $(a, b)_F$ is split.*
2. *The algebra $(a, b)_F$ is not a division algebra.*
3. *The norm map $N\colon (a, b)_F \to F$ has a nontrivial zero.*
4. *The element b is in the subgroup N_a.*

Proof. The implication (1) $\implies$ (2) is immediate from the definition of split, and (2) $\iff$ (3) is precisely the content of Proposition 1.10.

To prove (3) $\implies$ (4), we may assume that a is not a square in F. So, suppose that $v = v_0 + v_1i + v_2j + v_3ij$ is a nonzero quaternion with $0 = N(v) = v_0^2 - av_1^2 - bv_2^2 + abv_3^2$. That is, $(v_2^2 - av_3^2)b = v_0^2 - av_1^2$. Note that since a is not a square in F, we must have that $v_2^2 - av_3^2$ is nonzero. Thus

$$b = (v_0^2 - av_1^2)(v_2^2 - av_3^2)^{-1} \in N_a,$$

by Lemma 2.10.

Finally, we prove (4) $\implies$ (1). Again, we assume a is not a square in F. If $b \in N_a$ then $b^{-1} \in N_a$, hence there exist elements $r, s \in F$ such that $b^{-1} = r^2 - as^2$. Let $u := rj + sij$ and $v := (1 + a)i + (1 - a)ui$, we claim that $\{1, u, v, uv\}$ is a quaternionic basis of $(a, b)_F$.

We have

$$u^2 = r^2j^2 + s^2(ij)^2 - rsij^2 + rsij^2 = br^2 - abs^2 = b(r^2 - as^2) = bb^{-1} = 1.$$

Similarly, one can check that $v^2 = 4a^2$, and $uv = -vu$. Note that by Exercise 2.4, linear independence follows. However, we give a sketch of the details here using matrices of linear transformations. Observe that

$$\begin{aligned} 1 &= 1 + 0i + 0j + 0ij \\ u &= 0 + 0i + rj + sij \\ v &= 0 + (1+a)i - as(1-a)j - r(1-a)ij \\ uv &= 0 + (1-a)i - as(1+a)j - r(1+a)ij \end{aligned},$$

Thus the matrix of the transformation is

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1+a & 1-a \\ 0 & r & -as(1-a) & -as(1+a) \\ 0 & s & -r(1-a) & -r(1+a) \end{pmatrix},$$

and one computes that $\det(M) = 4ab^{-1} \neq 0$, hence M is invertible and $\{1, u, v, uv\}$ is a basis for $(a, b)_F$.

Thus the algebra $(a, b)_F$ is isomorphic to the algebra $(1, 4a^2)_F$ which is split by Proposition 2.5, as desired. □

Corollary 2.13

A quaternion algebra $(a, b)_F$ is either a division algebra over F or is isomorphic to $M_2(F)$.

Exercise 2.14. Let $a \in F^\times$ and consider the algebra $(a, -a)_F$ with standard quaternionic basis. Show that $(i + j)^2 = 0$. Use Theorem 2.12 to conclude that $(a, -a)_F \cong M_2(F)$.

Remark 2.15. *Since we have shown that $(a, b)_F \cong (b, a)_F$, all statements in Theorem 2.12 must be symmetric with respect to the parameters a and b. In particular, $b \in N_a$ if and only if $a \in N_b$. That is, the existence of a nontrivial solution to $b = x^2 - ay^2$ in F is equivalent to the existence of a nontrivial solution to $a = x^2 - by^2$ in F! In Lecture 3, we will introduce an alternative characterization of splitness from a geometric perspective, which makes this symmetry more readily apparent. Finally, if a is not a square in F, then $b \in N_a$ is equivalent to the statement that b is a norm from the extension $F(\sqrt{a})/F$.*

Key Takeaways

Square class dependence: The isomorphism class of $(a, b)_F$ depends only on the square classes of its parameters in $F^\times/F^{\times 2}$. Swapping or scaling basis elements reveals immediate structural equivalences, such as $(a, b)_F \cong (ac^2, bd^2)_F$.

A dichotomy: Every quaternion algebra over F is either a division ring or *split*, i.e., isomorphic to $M_2(F)$. The presence of even a single nonzero zero divisor forces the entire algebra to be isomorphic to a matrix ring over F!

Index

Bibliography

[Cona] Keith Conrad. The p-adic expansion of rational numbers. Expository notes. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/rationalsinQp.pdf.

[Conb] Keith Conrad. Quaternion algebras. Expository notes. URL: https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, Inc., Hoboken, NJ, 3rd edition, 2004.

[Gou20] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction*. Universitext. Springer, 3rd edition, 2020.

[GS17] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2nd edition, 2017. doi:10.1017/9781316661277.

[Han06] Andrew J. Hanson. *Visualizing Quaternions*. The Morgan Kaufmann Series in Interactive 3D Technology. Morgan Kaufmann, 2006.

[Hsu24] Catherine Hsu. Local fields. Lecture notes for the Preliminary Arizona Winter School (PAWS), 2024. URL: https://swc-math.github.io/aws/2025/PAWSHsu/2024PAWSHsuNotes.pdf.

[Kat07] Svetlana Katok. *p-adic Analysis Compared with Real*, volume 37 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2007.

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The Book of Involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface by J. Tits.

[Pol24] Paul Pollack. *Unreal Analysis: Visions of the p-adic Realm*. Ross Mathematics Program, 2024.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1973.

[Sil22] Joseph H. Silverman. *Abstract Algebra: An Integrated Approach*, volume 55 of *Pure and Applied Undergraduate Texts*. American Mathematical Society, Providence, Rhode Island, 2022.

[Voi21] John Voight. *Quaternion Algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, 2021. Available open access. doi:10.1007/978-3-030-56694-4.